Efficient-phase-encoding protocols for continuous-variable quantum key distribution using coherent states and postselection

Ryo Namiki*
CREST Research Team for Photonic Quantum Information,
Division of Materials Physics, Department of Materials Engineering Science,
Graduate school of Engineering Science, Osaka University, Toyonaka, Osaka 560-8531, Japan

Takuya Hirano
Department of Physics, Gakushuin University, Mejiro 1-5-1, Toshima-ku, Tokyo 171-8588, Japan
(Dated: February 1, 2008)

We propose efficient-phase-encoding protocols for continuous-variable quantum key distribution using coherent states and postselection. By these phase encodings, the probability of basis mismatch is reduced and total efficiency is increased. We also propose mixed-state protocols by omitting a part of classical communication steps in the efficient-phase-encoding protocols. The omission implies a reduction of information to an eavesdropper and possibly enhances the security of the protocols. We investigate the security of the protocols against individual beam splitting attack.

I. INTRODUCTION

In quantum key distribution (QKD), two distant parties, Alice and Bob share a secret key exploiting quantum channel and classical communication. By the laws of quantum physics the key can be proved to be secure against an eavesdropper (Eve) who has advanced technologies [1]. Many novel and modified QKD protocols have been proposed based on various theoretical and experimental aspects. For example, in the standard weak-coherent-state (WCS) implementation of the BB84 protocol, the transmission distance of QKD is limited by the photon-number-splitting (PNS) attack [2]. To defeat this limitation, modifications of the implementation have been proposed. An elegant one is the SARG protocol which changes the classical communication step in the implementation [3]. Another one is the decoy-state protocols that utilize fake signals to restrict possiblility of the PNS attack [4, 5].

A different type of WCS implementation has been proposed combining the idea of the balanced homodyne detection of an weak signal field with a strong field in the phase-encoding interferometric implementation of the BB84 protocol [6]. This proposal also includes the idea of postselection in continuous variable (CV) QKD. Following BB84, the protocol has inefficiency of basis mismatch associated with the random basis exchange, the choice of the quadratures. However, there are several CV QKD protocols that have no such inefficiency [7, 8, 9, 10]. In relation with the implementation, those protocols employ the amplitude modulations in addition to the phase modulation, and the signals are not necessarily WCS. Although CV QKD protocols are free from the limitation by the PNS attack, another practical limitation is given by the classical teleportation attack [11, 12].

In this paper we propose efficient phase-encoding protocols for CV QKD using balanced homodyne detection and postselection those have better efficiency than the original one [6] without significant changes in experimental setup. We also propose mixed-state protocols by omitting the part of classical communication steps.

In Sec. II, we review the original protocol and provide a basic notation. In Sec. III, we present modified protocols. In Sec. IV, we investigate the security against individual beam splitting attack. Sec. V is the conclusion and remarks.

II. ORIGINAL FOUR-COHERENT-STATE POSTSELECTION PROTOCOL

The original four-state postselection protocol (O4) [6, 13] is based on the phase-encoding interferometric implementation of QKD and the balanced homodyne detection of a weak signal field with a strong field as in FIG. 1.

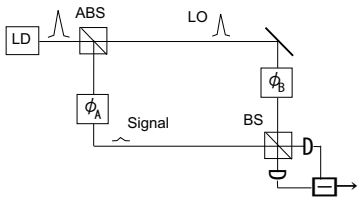

FIG. 1: The pulse emitted from a light source (LD) is split into a strong local oscillator (LO) and a weak signal field by an asymmetric beam splitter (ABS). Alice applies her phase shift ϕ_A to the signal and Bob applies his phase shift ϕ_B to the LO. The signal and LO interfere at the 50:50 beam splitter (BS). The difference between the photon numbers of the output pulses of the BS is observed.

Alice sends the coherent state $|\alpha e^{i\phi_A}\rangle$ with $\alpha > 0$ by randomly choosing her phase modulation ϕ_A from a set $\{0, \pi/2, \pi, 3\pi/2\}$. Bob measures the quadratures $\hat{x}(\phi_B) \equiv \hat{x}_1 \cos\phi_B + \hat{x}_2 \sin\phi_B$ by randomly choosing his phase modulation ϕ_B from a set $\{0, \pi/2\}$ where $\hat{x}_1 \equiv \frac{\hat{a}+\hat{a}^\dagger}{2}$ and $\hat{x}_2 \equiv \frac{\hat{a}-\hat{a}^\dagger}{2i}$. Bob's measurement is characterized by the quadrature distribution of the coherent state $|\langle x_{\phi_B}|\alpha e^{i\phi_A}\rangle|^2$ where $\langle x_{\phi_B}|$ is the eigenbra of $\hat{x}(\phi_B)$ with the eigenvalue x_{ϕ_B}. For a simpler notation we define

$$P(x, \alpha, \phi) \equiv \sqrt{\frac{2}{\pi}} \exp\left\{-2(x - \alpha\cos\phi)^2\right\}. \quad (1)$$

*Electric address: namiki@qo.phys.gakushuin.ac.jp

Then, we can write

$$|\langle x_{\phi_B}|\alpha e^{i\phi_A}\rangle|^2 = P(x_{\phi_B}, \alpha, \phi_A - \phi_B). \quad (2)$$

After the transmission, Bob informs Alice of his phase shift ϕ_B. If $|\phi_A - \phi_B| = \{0, \pi\}$, Bob's distribution is one of the Gaussian distributions centered either at $\pm\alpha$ as in FIG. 2. We call such a combination of (ϕ_A, ϕ_B) the *correct basis* and the quadrature distribution is given by

$$P_B(x, \alpha) = \frac{1}{2}\left(P(x, \alpha, 0) + P(x, \alpha, \pi)\right), \quad (3)$$

where x corresponds to Bob's measurement outcome.

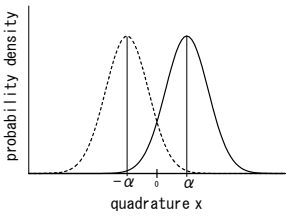

FIG. 2: The quadrature distributions of correct-basis choice are shown. The solid curve peaked at $x = \alpha$ corresponds to the signal of Alice's bit "1" and the dotted line peaked at $x = -\alpha$ corresponds to the signal of Alice's bit "0".

For the correct-basis case, the signal can transfer bit information from Alice to Bob by the following manner. Alice encodes her bit according to the combination of (ϕ_A, ϕ_B) as in Table I. Bob decodes the bit value according to his outcome x: If $x \geq 0$ his bit value is "1" otherwise his bit value is "0". The bit error rate (BER) conditioned on the absolute value $|x|$ is given by

$$q_B(x, \sqrt{\eta}\alpha) = \frac{P(|x|, \sqrt{\eta}\alpha, \pi)}{P(|x|, \sqrt{\eta}\alpha, 0) + P(|x|, \sqrt{\eta}\alpha, \pi)}. \quad (4)$$

where we assume the lossy channel with the line transmission η, $(0 < \eta \leq 1)$. Since the quadrature distributions are spread and overlapped, Bob's positive (negative) quadrature result needs not correspond to Alice's bit "1" ("0") and Bob's decoding has inherently finite errors. However, q_B is less than $\frac{1}{2}$ if $x \neq 0$ and non-zero information is transferred. By selecting the data according to the value of x, Alice and Bob can discard the erroneous portion. This process is called postselection.

If $(|\phi_A - \phi_B| \mod \pi) = \pi/2$, the signal is called the *wrong basis*. In this case, they cannot share the bit information because Bob's quadrature distribution is the same for such a combination of ϕ_A and ϕ_B, and the wrong-basis signal is discarded.

TABLE I: Alice's bit encoding of the original four-state protocol

ϕ_A	0	0	$\pi/2$	$\pi/2$	π	π	$3\pi/2$	$3\pi/2$
ϕ_B	0	$\pi/2$	0	$\pi/2$	0	$\pi/2$	0	$\pi/2$
$\langle\hat{x}\rangle$	α	0	0	α	$-\alpha$	0	0	$-\alpha$
A	1			1	0			0

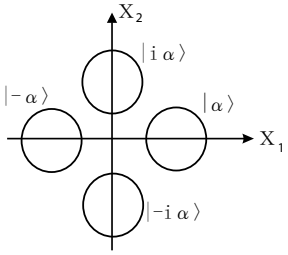

FIG. 3: Phase-space picture of the original four-state protocol

We define the efficiency P_e of the protocol as the probability that the signal becomes correct basis. In this O4 protocol one-half of signals are discarded and

$$P_e = \frac{1}{2}. \quad (5)$$

In the modified protocols, this quantity will be improved.

Alice's bit encoding of the O4 protocol associated with ϕ_A, ϕ_B, and Bob's mean value of quadratures $\langle\hat{x}\rangle \equiv \langle\alpha e^{i\phi_A}|\hat{x}(\phi_B)|\alpha e^{i\phi_A}\rangle$ is summarized in Table I where A represents Alice's bit. For the combination of wrong basis, $\langle\hat{x}\rangle$ is zero and A is set to be blank. The probability of wrong basis is determined by the number of blanks in the row A. A phase-space description is shown in FIG. 3.

Towards the modification, the essential point of performing the postselection is that Bob's distribution takes the form like FIG. 2. As we will show, the state configuration of FIG.3 and the random choice of a conjugate-quadrature pair is not necessary.

For a convenience, we set *Alice's bit encoding rule*: The combination of (ϕ_A, ϕ_B) that leads to $\langle\hat{x}\rangle = 0$ is for wrong basis, $\langle\hat{x}\rangle = \alpha$ is for bit "1" and $\langle\hat{x}\rangle = -\alpha$ is for bit "0". Note that Table I is consistent with this rule. We use this rule repeatedly in the following section.

The security of the protocol can be related to the uncertainty relation of the quadratures,

$$(\Delta x_1)^2(\Delta x_2)^2 \geq \frac{1}{16}. \quad (6)$$

Let us consider the ideal case, i.e., the channel and detector are lossless and noiseless. In such a case Bob can measure the mean and variance of $\hat{x}_1$ and $\hat{x}_2$ for each of the four coherent states and confirm that each of the states is in the minimum uncertainty state with $(\Delta x_1)^2 = (\Delta x_2)^2 = \frac{1}{4}$. Since such a minimum uncertainty state is a pure coherent state, this implies that a set of non-orthogonal states transfers without any disturbance. Thus, there is no Eve's intervention if the variances and mean values of quadratures have no changes, and the minimum uncertainty ensures the security.

III. EFFICIENT POSTSELECTION PROTOCOLS

In this section we present several modified protocols.

A. Three-state protocol

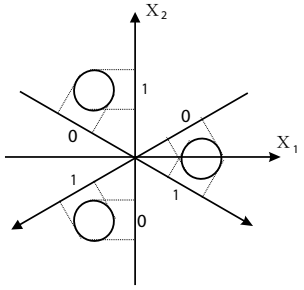

FIG. 4: Phase-space picture of the three-state protocol

The encoding of the three-state protocol is schematically described on the phasespace as in FIG. 4 (The "1"s and "0"s in FIG. 4 represent Alice's bit encoding associated with Bob's basis). Alice sends the coherent state $|\alpha' e^{i\phi_A}\rangle$ with $\phi_A = \{0, 2\pi/3, 4\pi/3\}$ and $\alpha' \equiv \frac{2}{\sqrt{3}}\alpha$. Bob measures $\hat{x}(\phi_B)$ with $\phi_B = \{\pi/2, -\pi/6, -5\pi/6\}$. We can easily see that if $(|\phi_A - \phi_B| \mod \pi)$ is different from $\pi/2$, then the quadrature distribution takes the form of the one in FIG. 2. In such a condition, we can perform the postselection procedure. If $(|\phi_A - \phi_B| \mod \pi) = \pi/2$, the combination of (ϕ_A, ϕ_B) is wrong basis and discarded.

Using Alice's bit encoding rule in Sec. II, we obtain Table II. From Table II, we can see that the wrong-basis case occurs with probability 1/3. Thus, the efficiency is

$$P_e = \frac{2}{3}, \tag{7}$$

which is 4/3 times higher than that of the O4 protocol.

TABLE II: Alice's bit encoding of the three-state protocol

ϕ_A	0	0	0	$2\pi/3$	$2\pi/3$	$2\pi/3$	$4\pi/3$	$4\pi/3$	$4\pi/3$
ϕ_B	$\pi/2$	$-\pi/6$	$-5\pi/6$	$\pi/2$	$-\pi/6$	$-5\pi/6$	$\pi/2$	$-\pi/6$	$-5\pi/6$
$\langle\hat{x}\rangle$	0	α	$-\alpha$	α	$-\alpha$	0	$-\alpha$	0	α
A		1	0	1	0		0		1

This encoding is based on the idea that Alice applies different encoding according to Bob's choice of basis. In CV QKD protocols, an efficient encoding where two variables are encoded on two conjugate quadratures has already been common. Our proposal can be interpreted as a generalization of this idea, namely, we encode two values on non-conjugate quadratures.

As a security aspect of the three-state protocol, it should be checked whether the minimum uncertainty is confirmed in the case Bob measures three different quadratures. Suppose that Bob observes $(\Delta x_2)^2 = \frac{1}{4}$ and $(\Delta x_\phi)^2 = \frac{1}{4}$. Then, from the definition of $\hat{x}(\phi)$,

$$\begin{aligned}(\Delta x_\phi)^2 &\equiv \langle(\hat{x}_1\cos\phi + \hat{x}_2\sin\phi)^2 - \langle\hat{x}_1\cos\phi + \hat{x}_2\sin\phi\rangle^2\rangle \\ &= (\Delta x_1)^2\cos^2\phi + (\Delta x_2)^2\sin^2\phi \\ &\quad + (\langle\hat{x}_1\hat{x}_2 + \hat{x}_2\hat{x}_1\rangle - 2\langle\hat{x}_1\rangle\langle\hat{x}_2\rangle)\sin\phi\cos\phi, \end{aligned} \tag{8}$$

TABLE III: Alice's bit encoding for the efficient four-state protocols

ϕ_A	$\pi/4$	$\pi/4$	$3\pi/4$	$3\pi/4$	$5\pi/4$	$5\pi/4$	$7\pi/4$	$7\pi/4$
ϕ_B	0	$\pi/2$	0	$\pi/2$	0	$\pi/2$	0	$\pi/2$
$\langle\hat{x}\rangle$	α	α	$-\alpha$	α	$-\alpha$	$-\alpha$	α	$-\alpha$
A	1	1	0	1	0	0	1	0

and we obtain

$$\left((\Delta x_1)^2 - \frac{1}{4}\right) + (\langle\hat{x}_1\hat{x}_2 + \hat{x}_2\hat{x}_1\rangle - 2\langle\hat{x}_1\rangle\langle\hat{x}_2\rangle)\tan\phi = 0. \tag{9}$$

Since this relation holds for both $\phi = -\pi/6$ and $\phi = -5\pi/6$ in the three-state protocol, we obtain

$$(\Delta x_1)^2 = \frac{1}{4}. \tag{10}$$

B. Efficient four-state protocols

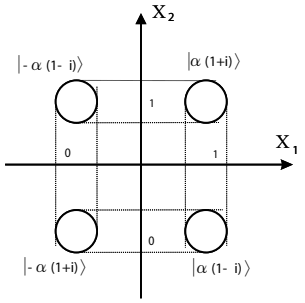

FIG. 5: Phase-space picture of the efficient four-state protocol

The encoding of the efficient four-state (E4) protocol is schematically described in FIG. 5. Alice sends $|\alpha'' e^{i\phi_A}\rangle$ with $\phi_A = \{\pi/4, 3\pi/4, 5\pi/4, 7\pi/4\}$ and $\alpha'' \equiv \sqrt{2}\alpha$. Bob measures $\hat{x}(\phi_B)$ with $\phi_B = \{0, \pi/2\}$. After the transmission (i) Bob informs Alice of his phase. Then, (ii) Alice tells Bob that her preparation of the states belongs to which one of the four sets $\{|\alpha'' e^{i\pi/4}\rangle, |\alpha'' e^{3i\pi/4}\rangle\}$, $\{|\alpha'' e^{3i\pi/4}\rangle, |\alpha'' e^{i5\pi/4}\rangle\}$, $\{|\alpha'' e^{5i\pi/4}\rangle, |\alpha'' e^{7i\pi/4}\rangle\}$, and $\{|\alpha'' e^{7i\pi/4}\rangle, |\alpha'' e^{i\pi/4}\rangle\}$ according to Bob's choice of the phase. Namely, if $\phi_B = 0$, Alice tells Bob that the state belong to either $\{|\alpha'' e^{i\pi/4}\rangle, |\alpha'' e^{3i\pi/4}\rangle\}$ or $\{|\alpha'' e^{5i\pi/4}\rangle, |\alpha'' e^{7i\pi/4}\rangle\}$. If $\phi_B = \pi/2$, Alice tells Bob that the state belong to either $\{|\alpha'' e^{3i\pi/4}\rangle, |\alpha'' e^{i5\pi/4}\rangle\}$ or $\{|\alpha'' e^{7i\pi/4}\rangle, |\alpha'' e^{i\pi/4}\rangle\}$.

In every case, the state takes the form similar to the one in FIG. 2 and we can perform the postselection procedure. Thus, the efficiency is

$$P_e = 1. \tag{11}$$

This is also clear from the configuration of the states in FIG. 5. Applying Alice's bit encoding rule we obtain Table III.

Now we present another four-state protocol by modifying the classical communication step of the E4 protocol. Let us

assume that Alice omits the announcement (ii), then the protocol still works without any further modification and the information that Alice and Bob share does not change. This is because Bob's distribution and bit decoding do not depend on the announcement (ii). The information is encoded on the pairs of the states, and it is not necessary to identify the states in each pair. Therefore, the redundant state information need not be announced.

This modification possibly enhances the security because Eve cannot exploit the classical information (ii). The loss of the information can be described by using the terms of mixed states. From Eve's point of view, Alice's preparation of states is not in a set of pure coherent states but in a set of mixtures of coherent states. We call this modified protocol the *mixed state protocol based on the four states* (MB4).

We have seen that the postselection protocol can be demonstrated without wrong-basis signal as in other CV QKD protocols. Conversely, if there are wrong-basis signals in a phase encoding CV QKD as in the O4 protocol, the signals are supposed to have some useful information and may play a role of the decoy states. Namely, the wrong-basis signals restrict Eve's possible operations. Such aspect has already been pointed out in Refs. [6, 13].

C. Six-state protocols

In a similar manner to the E4 and MB4 protocols, we can find a six-state protocol and its mixed-state version.

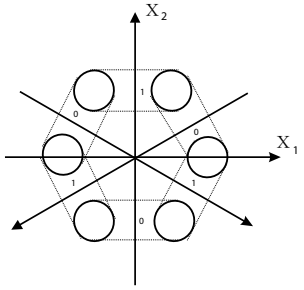

FIG. 6: Phase-space picture of the six-state protocol

The encoding of the six-state protocols can be schematically described on the phasespace as in FIG. 6. Alice sends $|\alpha' e^{i\phi_A}\rangle$ with $\phi_A = m\pi/3,\ m = \{0, 1, 2, \cdots, 5\}$. Bob measures $\hat{x}(\phi_B)$ with $\phi_B = \{\pi/2, -\pi/6, -5\pi/6\}$. The configuration of the six-state protocol in FIG. 6 has a similar symmetry to that of the three-state protocol in FIG. 4. If we make a mirror reflection of the three states associated with any one of the measured axes on the phasespace, we can obtain the six-state configuration.

From Fig. 6, we can see that if $(|\phi_A - \phi_B| \mod \pi)$ is different from $\pi/2$, the quadrature distribution takes the form similar to the one in Fig. 2. In such a condition, we can perform the postselection procedure. The other cases, i.e., $(|\phi_A - \phi_B| \mod \pi) = \pi/2$, are for wrong-basis result.

Using the bit encoding rule, we can obtain Table IV. From Table IV, we can see that the efficiency is

$$P_e = \frac{2}{3}, \tag{12}$$

which is equivalent to that of the three-state protocol.

TABLE IV: Alice's bit encoding of the six-state protocols

ϕ_A	0	0	0	$\pi/3$	$\pi/3$	$\pi/3$	$2\pi/3$	$2\pi/3$	$2\pi/3$	π	π	π	$4\pi/3$	$4\pi/3$	$4\pi/3$	$5\pi/3$	$5\pi/3$	$5\pi/3$
ϕ_B	$\pi/2$	$-\pi/6$	$-5\pi/6$	$\pi/2$	$-\pi/6$	$-5\pi/6$	$\pi/2$	$-\pi/6$	$-5\pi/6$	$\pi/2$	$-\pi/6$	$-5\pi/6$	$\pi/2$	$-\pi/6$	$-5\pi/6$	$\pi/2$	$-\pi/6$	$-5\pi/6$
$\langle\hat{x}\rangle$	0	α	$-\alpha$	α	0	$-\alpha$	α	$-\alpha$	0	0	$-\alpha$	α	$-\alpha$	0	α	$-\alpha$	α	0
A		1	0	1		0	1	0			0	1	0		0	0	1	

The classical communication step in the six-state protocol is as follows: (i) Bob informs Alice of his phase ϕ_B and then (ii) Alice tells Bob that her preparation of the states is wrong basis or belongs to either two-state subset in the one of the three sets

$$\left\{\{|\alpha' e^{i\pi/3}\rangle, |\alpha' e^{5i\pi/3}\rangle\}, \{|\alpha' e^{2i\pi/3}\rangle, |\alpha' e^{4i\pi/3}\rangle\}\right\}, \tag{13}$$

$$\left\{\{|\alpha'\rangle, |\alpha' e^{2i\pi/3}\rangle\}, \{|\alpha' e^{i\pi}\rangle, |\alpha' e^{5i\pi/3}\rangle\}\right\}, \tag{14}$$

and

$$\left\{\{|\alpha' e^{i\pi/3}\rangle, |\alpha' e^{i\pi}\rangle\}, \{|\alpha'\rangle, |\alpha' e^{4i\pi/3}\rangle\}\right\}, \tag{15}$$

according to the value of $\phi_B = \pi/2, -\pi/6$, and $-5\pi/6$, respectively.

Let us modify the step (ii) as (ii)$'$ Alice tells Bob that her preparation of the states is wrong basis or not. Then, the protocol still works and the performance is essentially the same. This provides the *mixed state protocol based on the six states* (MB6). In this protocol, Alice's preparation of states is considered to be one of the equal-probability mixtures of the states in one of the subsets.

Note that all above protocols can be performed essentially in the same experimental setup based on the interferometer because the modifications are given in the way of phase modulation and classical communication steps.

D. Eight-state protocols

We describe an eight-state protocol and its mixed-state version. Different from the previous ones, this protocol requires not only the phase modulation, but also the amplitude modulation in the interferometric implementation.

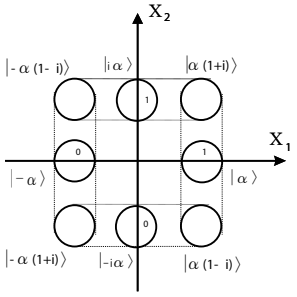

FIG. 7: Phase-space picture of the eight-state protocol

The encoding of the eight-state protocols can be schematically described on the phasespace as in FIG. 7. Alice sends coherent state $\{|\alpha e^{i\frac{m}{2}\pi}\rangle, |\alpha'' e^{i\frac{2m'+1}{4}\pi}\rangle\}$ by choosing $\phi_A = m\pi/2, m = \{0,1,2,3\}$ with α and $\phi_A = (2m'+1)\pi/4, m' = \{0,1,2,3\}$ with $\alpha'' = \sqrt{2}\alpha$. Bob chooses his phase $\phi_B = \{0, \pi/2\}$.

From FIG. 7, we can see that if $(|\phi_A - \phi_B| \mod \pi)$ is different from $\pi/2$, the quadrature distribution takes the form similar to the one in FIG. 2. In such a condition, we can perform the postselection procedure. The other cases, i.e., $(|\phi_A - \phi_B| \mod \pi) = \pi/2$, are for wrong-basis result. Using the bit encoding rule, we can obtain Table V. From Table V, we can see that the efficiency is

$$P_e = \frac{3}{4} \tag{16}$$

which is higher than that of the O4 protocol by the factor of 3/2.

TABLE V: Alice's bit encoding of the eight-state protocol

ϕ_A	0	0	$\pi/4$	$\pi/4$	$\pi/2$	$\pi/2$	$3\pi/4$	$3\pi/4$	π	π	$5\pi/4$	$5\pi/4$	$3\pi/2$	$3\pi/2$	$7\pi/4$	$7\pi/4$
ϕ_B	0	$\pi/2$	0	$\pi/2$	0	$\pi/2$	0	$\pi/2$	0	$\pi/2$	0	$\pi/2$	0	$\pi/2$	0	$\pi/2$
$\langle\hat{x}\rangle$	α	0	α	α	0	α	$-\alpha$	α	α	$-\alpha$	0	$-\alpha$	$-\alpha$	0	α	$-\alpha$
A	1		1	1		1	0	1	0	0		0	0		1	0

In the classical communication step, (i) Bob informs Alice of his phase ϕ_B and then (ii) Alice tells Bob that her preparation of the states is wrong basis or belongs to which one of the two-state subsets in the two sets

$$\left\{\{|\alpha\rangle, |\alpha e^{i\pi}\rangle\}, \{|\alpha'' e^{i\pi/4}\rangle, |\alpha'' e^{3i\pi/4}\rangle\}, \{|\alpha'' e^{5i\pi/4}\rangle, |\alpha'' e^{7i\pi/4}\rangle\}\right\}, \tag{17}$$

and

$$\left\{\{|\alpha e^{i\pi/2}\rangle, |\alpha e^{3i\pi/2}\rangle\}, \{|\alpha'' e^{i\pi/4}\rangle, |\alpha'' e^{7i\pi/4}\rangle\}, \{|\alpha'' e^{3i\pi/4}\rangle, |\alpha'' e^{5i\pi/4}\rangle\}\right\}, \tag{18}$$

according to the value of $\phi_B = 0$, and $\pi/2$, respectively.

Let us modify the process (ii) as (ii)$'$ Alice tells Bob that

her preparation of the states is wrong basis or not. Then, still the protocol works and the performance is essentially the same. In this case, Alice's preparation of states is considered to be a three-state equal-probability mixture. We call this modified eight-state protocol the *mixed state protocol based on the eight states* (MB8). The MB8 protocol is considered to be a mixture of the O4 and E4 protocols with certain changes in the classical communication step. Thus, it is possible to switch the protocols by changing the classical communication after the transmission.

E. Generalization of protocols

We present a generalized mixed-state protocol which includes the MB4 and MB8 protocols. This generalization may not have practical utility but it is useful for the discussion of the security (see Sec. IV).

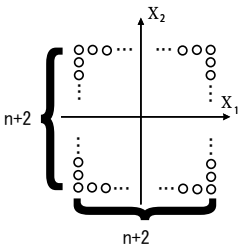

FIG. 8: Phase-space picture of the $4n+4$-state protocol

The encoding of the generalized protocol can be schematically described on the phasespace as in FIG. 8. Alice randomly sends one of the $4n+4$ states, $|\alpha(\pm 1 + i(\frac{2k}{n+1} - 1))\rangle$, $|\alpha(\pm i + (\frac{2m}{n+1} - 1))\rangle$, $k = 0, 1, 2, \cdots, n+1$, $m = 1, 2, \cdots, n$. Bob measures one of the quadratures, $\hat{x}_1$ or $\hat{x}_2$.

Alice encodes bit "1" for $|\alpha(1 + i(\frac{2k}{n+1} - 1))\rangle$ and "0" for $|\alpha(-1 + i(\frac{2k}{n+1} - 1))\rangle$ in the case that Bob measures $\hat{x}_1$. Alice encodes bit "1" for $|\alpha(i + (\frac{2k}{n+1} - 1))\rangle$ and "0" for $|\alpha(-i + (\frac{2k}{n+1} - 1))\rangle$ in the case that Bob measures $\hat{x}_2$. The other cases are discarded. In this protocol, Alice's preparation of states is considered to be a $n+2$-state equal-probability mixture. We can see that $n = 0$ corresponds to the MB4 protocol and $n = 1$ correspond to the MB8 protocol. The efficiency is given by

$$P_e = \frac{2+n}{2+2n}. \tag{19}$$

IV. SECURITY AGAINST INDIVIDUAL BEAM SPLITTING ATTACK

A. Individual beam splitting attack

The safety of the QKD protocols under lossy channel is estimated by assuming the beam splitting attack where Eve replaces the lossy channel with lossless one and splits the portion of signal corresponds to the loss. Here we consider the individual beam splitting attack where Eve stores the portion for arbitrarily long time with a perfect quantum memory and she performs her measurement on individual signal independently after she learns Bob's basis of each signal.

In the present protocols, Alice's preparation of states is represented by the form of the coherent-state mixture

$$\hat{\rho}(p_i, \alpha_i) = \sum_i p_i |\alpha_i\rangle\langle\alpha_i| \tag{20}$$

The states of Bob and Eve under the beam splitting attack are given by $\hat{\rho}(p_i, \sqrt{\eta}\alpha_i)$ and $\hat{\rho}(p_i, \sqrt{1-\eta}\alpha_i)$ respectively, where η is the line transmission ($0 < \eta \leq 1$).

B. Eve's knowledge

Let us assume the situation that Eve receives one of the binary states $\hat{\rho}_\pm$ whose subscript corresponds to Alice's bit encoding and each of them appears with the equal probability, $\frac{1}{2}$. An upperbound of Eve's knowledge represented by the fraction of the bit sequence deleted in the privacy amplification [14, 15, 16] is given by

$$\tau_u \;=\; \log_2(2 - |\langle\psi_+|\psi_-\rangle|^2), \tag{21}$$

where $|\psi_\pm\rangle$ is a purification of $\hat{\rho}_\pm$. This formula is originally given for the pure-state signal [17]. For the case of the mixed-state signal, by assuming Eve obtains a purification that always includes the original mixed-state signal, we can safely estimate an upperbound. A tight estimation of the inner product is directly calculated by the fidelity [18]

$$F(\hat{\rho}_+, \hat{\rho}_-) \;=\; \max_{|\psi_\pm\rangle} |\langle\psi_+|\psi_-\rangle| = \mathrm{Tr}\sqrt{\sqrt{\hat{\rho}_+}\hat{\rho}_-\sqrt{\hat{\rho}_+}} \tag{22}$$

where the maximization is taken over all the purifications.

In the following we determine Eve's states under the beam splitting attack for each of the protocols and estimate the inner product $|\langle\psi_+|\psi_-\rangle|$. It is shown that all of them have the same bound of the inner product $|\langle\psi_+|\psi_-\rangle| = e^{-2(1-\eta)\alpha^2}$, which gives the same upperbound of Eve's knowledge.

For the three-state protocol, Eve's states are given by

$$\hat{\rho}_\pm = |\sqrt{1-\eta}\alpha' e^{\pm\frac{2}{3}\pi}\rangle\langle\sqrt{1-\eta}\alpha' e^{\pm\frac{2}{3}\pi}| \tag{23}$$

assuming that Bob set $\phi_B = \pi/2$. Then, taking $|\psi_\pm\rangle = |\sqrt{1-\eta}\alpha' e^{\pm\frac{2}{3}\pi}\rangle$, we obtain $|\langle\psi_+|\psi_-\rangle| = e^{-2(1-\eta)\alpha^2}$. The same bound can be applied for $\phi_B = -\pi/6$ and $\phi_B = -5\pi/6$ because in that case $\hat{\rho}_\pm$ can be obtained from those in Eq. (23) with proper rotations in the phasespace. Similarly we omit the discussions of phase-covariant cases in the followings. Since the configuration of the six-state protocols can be obtained from that of the three-state protocol by the mirror reflection. The same bound can be applied to the pure version of the six-state protocols.

For the E4 protocol, Eve's states are given by

$$\hat{\rho}_\pm \;=\; |\sqrt{1-\eta}(1 \pm i)\alpha\rangle\langle\sqrt{1-\eta}(1 \pm i)\alpha| \tag{24}$$

assuming that Bob set $\phi_B = \pi/2$ and Alice announced her preparation was in the pair $|(1 \pm i)\alpha\rangle$. Then, taking $|\psi_\pm\rangle = |(1 \pm i)\alpha\rangle$ we obtain the same bound, $|\langle\psi_+|\psi_-\rangle| = e^{-2(1-\eta)\alpha^2}$.

For the MB4 protocol, Eve's states are given by

$$\begin{aligned}\hat{\rho}_\pm \;=\; \frac{1}{2}\Big(&|\pm\sqrt{1-\eta}(1+i)\alpha\rangle\langle\pm\sqrt{1-\eta}(1+i)\alpha| \\ &+|\pm\sqrt{1-\eta}(1-i)\alpha\rangle\langle\pm\sqrt{1-\eta}(1-i)\alpha|\Big)\end{aligned} \tag{25}$$

assuming that Bob set $\phi_B = 0$. Using the formula of the fidelity in Appendix **A**, we obtain the estimation $F = e^{-2(1-\eta)\alpha^2}$. Since Eve's states of the pure version of the eight-state protocols is that of either the O4 protocol or the E4 protocol. Therefore, the pure version of the eight-state protocols also has the same bound.

For the MB6 protocol, Eve's states are given by

$$\hat{\rho}_\pm = \frac{1}{2}\Bigg(|\sqrt{1-\eta}\alpha' e^{\pm\frac{\pi}{3}}\rangle\langle\sqrt{1-\eta}\alpha' e^{\pm\frac{\pi}{3}}| + |\sqrt{1-\eta}\alpha' e^{\pm\frac{2}{3}\pi}\rangle\langle\sqrt{1-\eta}\alpha' e^{\pm\frac{2}{3}\pi}| \Bigg) \quad (26)$$

assuming that Bob set $\phi_B = \pi/2$. Then, using the formula of the fidelity in Appendix **A** again, we obtain the estimation $F = e^{-2(1-\eta)\alpha^2}$.

For the generalized protocol including the MB4 and MB8 protocol, Eve's states are given by

$$\hat{\rho}_\pm \equiv \frac{1}{n+2}\sum_{k=0}^{n+1} |\beta_\pm(n,k)\rangle\langle\beta_\pm(n,k)|, \quad (27)$$

$$\beta_\pm(n,k) \equiv \sqrt{1-\eta}\alpha\left\{\pm 1 + i\left(\frac{2k-n-1}{n+1}\right)\right\}, \quad (28)$$

assuming Bob set $\phi_B = 0$. We can see that the following states are purifications of $\hat{\rho}_\pm$,

$$|\psi_\pm\rangle \equiv \frac{1}{\sqrt{n+2}}\sum_{k=0}^{n+1} |\beta_\pm(n,k)\rangle|k\rangle e^{\pm i\omega(k)}, \quad (29)$$

$$\omega(k) \equiv (1-\eta)\alpha^2\left(\frac{2k-n-1}{n+1}\right), \quad (30)$$

where $\{|k\rangle\}$ is an orthonormal basis set of an extended space. The bound is given by

$$|\langle\psi_+|\psi_-\rangle| = e^{-2(1-\eta)\alpha^2} \quad (31)$$

independent of n.

The purification $|\psi_\pm\rangle$ of Eq. (29) implies that Eve knows the extra-state information k which is never announced in the mixed-state protocols. Given this information Eve's problem is just to distinguish the two pure states $|\beta_\pm(n,k)\rangle$. Thus, the bound is equal to that of the pure-state case. In this sense, the information from the mixed-state signal is upper bounded by that of the pure-state case and the omission of the classical communication possibly reduces Eve's information. This fact suggests that mixed-state protocols are advantageous. However, optimization problems for mixed-state signals are technically difficult compared with those for pure-state cases in general. For the pure-state protocols, the upperbound is achievable by the optimal measurement which minimizes the error rate. On the other hand, it is not sure that the upperbound can be tight for the mixed-state protocols. If the bound is not tight, it implies that the mixed-state protocol is more secure.

C. Formula of secure key gain

The secure key gain [14, 15, 16] as a estimation of QKD performance against individual BS attack for the present protocols is given by

$$G(\alpha,\eta,x_0) = P_e\left(\sum_x P_B(x,\sqrt{\eta}\alpha) i(q_B(|x|,\sqrt{\eta}\alpha)) - \tau_u\right) \quad (32)$$

where

$$i(q) \equiv 1 + q\log_2 q + (1-q)\log_2(1-q) \quad (33)$$

is the mutual information of the binary symmetric channel, and $\tau_u = \log_2(2 - e^{-4(1-\eta)\alpha^2})$ is given from the previous subsection. Since the correct-basis distributions, the BER, and τ are the same as those of the O4 protocol, the value of the gain is the same as that of the O4 protocol [11] except for the factor P_e.

In the presence of noise, the estimation of the gain is in progress. As long as we use the coherent states and homodyne detection the limitation of all the protocols can be found [11, 12].

V. CONCLUSION AND REMARKS

We have proposed several phase-encoding protocols for quantum key distribution using coherent states and postselection. The modified phase encodings reduce the probability of wrong basis and increase the efficiency. The proposed protocols include the mixed-state protocols, those are obtained from the protocols exploiting more than three states by omitting the annoucement of the redundant state information in the classical communication steps.

We have investigated the security of the protocols against the individual beam splitting attack. We showed that the improvement of the key gains is simply proportional to the efficiency and no substantial difference is observed whether the protocol is mixed-state version or not. This result is depending on the way of our analysis and it leaves an open question whether the modified protocols provide physically different condition in the security of QKD particularly on the relation with the introduction of the mixed states.

There exist several possibilities to make other protocols. Trivial one is to increase the way of phase modulations. To use asymmetric configuration or biased choice of basis [19] may be interesting. Extensive search of protocols and optimization of efficiencies are left for future works.

APPENDIX A: FIDELITY BETWEEN THE MIXTURES OF TWO COHERENT STATES

We derive a formula of the fidelity between the mixtures of two coherent states

$$\hat{\rho} = \frac{1}{2}\left(|\alpha\rangle\langle\alpha| + |\beta\rangle\langle\beta|\right) \quad (A1)$$

$$\hat{\sigma} = \frac{1}{2}\left(|-\alpha\rangle\langle-\alpha| + |-\beta\rangle\langle-\beta|\right) \quad (A2)$$

with $\alpha = a + ib, \beta = a - ib, (a, b \geq 0)$. A phase-space configuration of the states is shown in FIG. 9. Since we can write

$$\sqrt{\hat{\rho}} = \frac{1}{\sqrt{2}}\left(\sqrt{1+\gamma}|+\rangle\langle+| + \sqrt{1-\gamma}|-\rangle\langle-|\right) \quad (A3)$$

where we defined an orthonormal basis which diagonalizes $\hat{\rho}$

$$|\pm\rangle \equiv \frac{|\alpha\rangle \pm e^{i\phi}|\beta\rangle}{\sqrt{2(1\pm\gamma)}} \quad (A4)$$

$$\gamma e^{i\phi} \equiv \langle\beta|\alpha\rangle, \gamma \geq 0, \quad (A5)$$

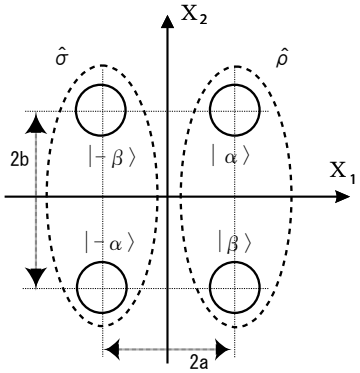

FIG. 9: Phase-space picture of the mixtures of two coherent states

we can find a matrix representation of $\sqrt{\hat{\rho}}\hat{\sigma}\sqrt{\hat{\rho}}$ as

$$\begin{pmatrix} \langle +| \\ \langle -| \end{pmatrix} \sqrt{\hat{\rho}}\hat{\sigma}\sqrt{\hat{\rho}} \begin{pmatrix} |+\rangle & |-\rangle \end{pmatrix} \equiv \frac{1}{4}\begin{pmatrix} (1+\gamma)\langle +|\hat{\sigma}|+\rangle & \sqrt{1-\gamma^2}\langle +|\hat{\sigma}|-\rangle \\ \sqrt{1-\gamma^2}\langle -|\hat{\sigma}|+\rangle & (1-\gamma)\langle -|\hat{\sigma}|-\rangle \end{pmatrix}$$
$$= \frac{e^{-4a^2}}{4}\begin{pmatrix} 1+e^{-4b^2}+2e^{-2b^2}\cos(4ab) & -2ie^{-2b^2}\sin(4ab) \\ 2ie^{-2b^2}\sin(4ab) & 1+e^{-4b^2}-2e^{-2b^2}\cos(4ab) \end{pmatrix}. \quad \text{(A6)}$$

Then, using the relation $\mathrm{Tr}\sqrt{X} = \sqrt{\mathrm{Tr}X + 2\sqrt{\det X}}$ for a 2×2 positive matrix X, we obtain the fidelity

$$F(\hat{\rho},\hat{\sigma}) \equiv \mathrm{Tr}\sqrt{\sqrt{\hat{\rho}}\hat{\sigma}\sqrt{\hat{\rho}}} = \sqrt{\mathrm{Tr}(\sqrt{\hat{\rho}}\hat{\sigma}\sqrt{\hat{\rho}}) + 2\sqrt{\det(\sqrt{\hat{\rho}}\hat{\sigma}\sqrt{\hat{\rho}})}} = e^{-2a^2}. \quad \text{(A7)}$$

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74,** 145 (2002).
[2] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85,** 1330 (2000).
[3] V.Scarani, A. Aci'n, G. Ribordy, and N. Gisin Phys. Rev. Lett. **92,** 057901 (2004).
[4] W.-Y. Hwang, Phys. Rev. Lett. **91,** 057901 (2003).
[5] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94,** 230504 (2005).
[6] T. Hirano, H. Yamanaka, M. Ashikaga, T. Konishi, and R. Namiki, Phys. Rev. A **68,** 042331 (2003).
[7] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88,** 057902 (2002).
[8] Ch. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs, Phys. Rev. Lett. **89,** 167901 (2002).
[9] F. Grosshans, G.V. Assche, J. Wenger, R. Brouri, N.J. Cerf, and P. Grangier, Nature 421, 238 (2003).
[10] C. Weedbrook, A. M. Lance, W.P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, Phys. Rev. Lett. **93,** 170504 (2004).
[11] R. Namiki and T. Hirano, Phys. Rev. Lett. **92,** 117901 (2004)
[12] R. Namiki and T. Hirano, Phys. Rev. A **72,** 024301 (2005).
[13] R. Namiki and T. Hirano, Phys. Rev. A **67,** 022308 (2003).
[14] N. Lütkenhaus, Phys. Rev. A **54,** 97 (1996).
[15] N. Lütkenhaus, Phys. Rev. A **59,** 3301 (1999).
[16] N. Lütkenhaus, Phys. Rev. A **61,** 052304 (2000).
[17] B. A. Slutsky, R. Rao, P. Sun, and Y. Fainman, Phys. Rev. A **57,** 2383 (1998).
[18] M.A. Nielsen and I.L. Chuang, *Quantum Computation and Quantum Information* (Cambridge, 2000).
[19] H.-K. Lo, H.F. Chau, and M. Ardehali, J. of Cryptology, **18,** 133-165, (2005); quant-ph/0011056.